Computer & Communications Industry Association
Tech Advocacy Since 1972

Statement of

Alyssa Doom
State Policy Director
Computer & Communications Industry Association

Regarding

Pre-Rulemaking Stakeholder Sessions
California Privacy Protection Agency

May 4, 2022

Chair Urban and Members of the California Privacy Protection Agency:

Thank you for the opportunity to provide input on the upcoming rulemaking under the California Privacy Rights Act, or "CPRA". My name is Alyssa Doom and I am speaking today on behalf of the Computer and Communications Industry Association, or "CCIA". CCIA is a nonprofit, nonpartisan trade association that for 50 years has represented a broad cross section of small, medium, and large communications and technology firms. Our members place high value on the protection of individual privacy and support the important principles that underpin the CPRA, including transparency, accountability, and consumer control over how their data is processed and used.

CCIA has long supported enactment of comprehensive federal baseline privacy legislation to avoid the creation of a divergent set of state privacy laws that could result in a confusing and burdensome regulatory patchwork. However, we understand that in the absence of a federal regime, state lawmakers have a continued interest in enacting local privacy policies to protect consumers. As such, the Association has proposed a set of state privacy principles to inform legislators as local legislation is considered. Among these is the need to adopt a risk-based approach to privacy protections. My brief comments will focus on the importance of adopting a risk-based model for regulating the use of automated decision-making tools.

CCIA recommends that rules concerning automated decision-making focus on securing protections for consumers with respect to decisions that are *fully automated* and that may have *legal or similarly significant effects*. The rules should not create unnecessary restrictions for low-risk systems and tools that support ordinary business operations and transactions. We advise that regulations involving automated decision-making reflect the following principles governing regulatory terminology, access to meaningful information, and consumer opt-outs.

1. **Regulatory Terminology**

I will first focus on regulatory terminology. The regulation of "automated decision-making" is an emerging concept in privacy law and, as such, the term lacks clear, universally accepted legal definitions. Under the CPRA, the term "automated decision-making" could be interpreted so broadly as to encompass a range of low-risk processing activities and basic tools that have proven beneficial for both businesses and consumers, such as spreadsheets or spell-checkers. The term could even reach the automated tools Internet companies rely on to responsibly moderate their services and keep their users safe, such as chat, spam, and abuse filters. The adoption of overly inclusive regulatory terminology could impede the use of such widely accepted tools. Therefore, we recommend that the regulations ensure that businesses shall only be obligated to implement access or opt-out requests with respect to fully automated decisions involving personal information having legal or similarly significant effects, such as processing that impacts access to medical treatment, public assistance, or credit decisions.

2. **Access to Information About Automated Decisions**

Next, I will turn to potential regulations governing consumers' access to information about automated decision-making. Again, CCIA recommends that the forthcoming regulations focus on high-risk automated decision-making processing. Here, the Agency should provide guidance on how to develop notices that contain clear information regarding the purpose of the high-risk automated processing and the source, categories, and relevance of the processed information. Companies should be able to make these disclosures through existing websites and transparency notices. Explanations should be straightforward, allowing users to understand the impacts of the automated decision-making on their lives. Importantly, the degree to which businesses will be required to disclose this information should be proportionate to the level of risk associated with the automated decisions and should not implicate trade secrets or business sensitive information. Disclosures should only be required in connection with automated decisions that produce legal or similarly significant effects for consumers. An obligation to provide disclosures for each type of low-risk automated decision would overwhelm businesses and have no clear benefit to consumers. In addition, and equally important, regulations should not require businesses to disclose trade secrets or proprietary information such as algorithms or source code. These types of disclosures are unlikely to provide meaningful protections against risk, are of little practical use to consumers, and can severely chill not only the provision of good customer service but also innovation and speech.

3. ***Opt-Out Rights With Respect to Automated Decisions***

Finally, consistent with emerging U.S. privacy regimes, only fully automated decisions that produce legal or similarly significant effects should be subject to rules establishing consumer opt-out rights. To provide greater legal certainty, regulations should specify the categories of use cases that would be implicated here – such as decisions that result in the provision or denial of financial or lending services or access to essential goods or services. Broader applicability to low-risk decisions would impede ordinary business activity and diminish the availability and functionality of personalized consumer services. Lastly, in instances where high-risk automated decision-making processing is essential to provide certain services or where a core function of the service is its

automation, businesses should be able to demonstrate to consumers supplemental precautions taken instead of offering opt-out options.

***

In sum, requiring prescriptive, one-size fits all privacy controls that cover the processing of non-sensitive or de-identified data would be inconsistent with consumer expectations, degrade user experience, and hinder legitimate business practices. We believe the Agency can mitigate these pitfalls, while upholding privacy protections, by promulgating regulations with these principles in mind.

CCIA welcomes the thoughtful and deliberative approach taken by the Agency in considering the key operational and enforcement issues introduced or modified by the CPRA. I will also be submitting these remarks in a written format alongside CCIA's State Privacy Principles and invite Members to contact me following the hearing should questions arise.